itworldcanada.com

Understanding current cybersecurity challenges in law: determining online jurisdictional authority (Article 3) - IT World Canada

Melissa Lukings and Arash Habibi Lashkari

14-18 minutes

When a crime takes place or a dispute occurs between two parties who reside within the same geographic location, the determination of which law applies to that scenario is easily distinguished as being the law of that geographic location. When a dispute occurs between two parties who reside in different nations – or legal jurisdictions – the methodology for determining which country's laws and legal forum should apply is rooted in the topics of private international law, international criminal law, and conflicts of law. While these topics are by no means straightforward or simple, the strategy for addressing legal disputes or criminal offences which occur between or across legal jurisdictions becomes greatly complexified when the alleged crime, dispute, or other offence takes place online or is otherwise enabled via the internet.

Previously in this series, we have discussed the concept of data sovereignty as a challenge in our global digital world as it relates both to law and to cybersecurity and examined the complex issue

of cross-border data transfers. We have also examined the concept of digital governance, governance strategies, and the relation between digital governance, data sovereignty, and law around the world. You can view our previous articles here:

Understanding Current Cybersecurity Challenges in Law: Digital Governance and Social Responsibility Meet User-Generated Content (Article 2)

Understanding Current Cybersecurity Challenges in Law: Data Sovereignty and Cross-Border Data Transfers (Article 1)

This is the third article in our six-part series. In this article, we will discuss the complexities of determining jurisdiction in international law, with a specific emphasis on cybercrime and issues pertaining to internet law which occur between legal jurisdictions.

Jurisdiction

Jurisdiction refers to the power, the right, or the authority to interpret and apply the law. Jurisdiction can also refer to a specific regional, physical, territorial, or geographic area in more casual terms.

While jurisdiction is often linked to sovereignty over a territorial location, jurisdiction can also exist without a connection to territory. The type of jurisdictional authority held by a governing body indicates whether that nation or state can undertake enforcement action to uphold its law. This becomes more complex when we consider online activities, particularly cybercrimes, defamation, and other tortious activities, as there may not necessarily be a defined geographic area to distinguish which governing authority has the legal jurisdiction to address these matters.

The court of jurisdiction refers to which court has the right or the power to hear a case or argument and render a judgment. It is important, when deciding on a court of jurisdiction, to determine which type of matter the court will hear, as each type of court hears only certain types of arguments or cases. For example, in matters of national law, a federal court would be the appropriate court, as it has legal jurisdiction over matters on a national level. Conversely, minor civil matters may be heard in small claims, civil, or municipal courts, family courts handle matters of family law, criminal courts handle criminal matters, and appeal courts handle appeals of previous judgements made in lower courts.

Jurisdictional authority

In legal systems, jurisdictional authority refers to the practical legal authority to make, enforce, and administer laws and justice, which is granted to a legal body based on the type and locational circumstances of the case. There are three main types of jurisdictional authority that grant courts legal power over certain matters: prescriptive jurisdiction, enforcement jurisdiction, and adjudicative jurisdiction.

Prescriptive jurisdiction refers to the authority of the governing body of a nation or state to establish laws and legal norms that are applicable to individuals, groups, corporations, property, and events, both within and outside of its territory. Under the prescriptive jurisdiction, the laws of a nation or state are still binding on citizens of that jurisdiction while abroad. The same principle of legal scope may also be applicable to certain events or activities conducted abroad that could negatively impact the nation or state which is hoping to assert a prescriptive jurisdiction. For

example, a nation may choose to create legislation applicable to crimes that occur abroad which the home nation considers to be a threat to its security or economic interests.

Enforcement jurisdiction refers to the power of a nation or state to ensure compliance with prescriptive legal commands which regulate people and situations in the jurisdiction of that nation or state. Enforcement jurisdiction is closely tied to the adjudicative jurisdiction and both can be contrasted with the prescriptive jurisdiction.

Adjudicative jurisdiction refers to the power of the governing body of a nation or state to hear and settle legal disputes, as well as the authority to decide and determine the outcomes of competing legal claims. Both the adjudicative jurisdiction and enforcement jurisdiction are territorially limited. The intention for this is to limit the power of a nation or state to enforce its prescriptive or adjudicative jurisdiction within another nation or state. In this way, the legal enforcement and court systems are restricted to operating within the territorial boundaries of their corresponding nation or state. In the absence of permission, a nation or state cannot exercise its prescriptive jurisdiction—either through enforcement or adjudication—outside of its territory.

Determining jurisdictional authority

There are three factors to consider when determining the appropriate court to hear a legal matter, both domestically and on an international level. These correspond with the three types of jurisdictional authority and include: jurisdiction of law, recognition of law, and enforcement of law.

1. **Legal Jurisdiction** – *Does the court have the judicial (or legal) power over both the person going on trial and the type of matter that is being tried?*
2. **Legal Recognition** – *Will a decision by the court be accepted (or recognized) in foreign countries and/or other jurisdictions?*
3. **Legal Enforcement** – *Does the court have the power to instil (or enforce) the punishment that is being sought out in this matter?*

Domestically, when a corporation exists within a nation and does business between different regional jurisdictions, the courts may look for evidence of the intent of the corporation to do business in one region in contrast to its presence in another. Evidence of intent to do business may be proved through various means, including contractual agreements, targeted sales, advertising campaigns, or some types of contact made within another region. Online, such contact could be that which is made by the operators of a website with businesses in a specific geographic area via the availability of the website itself. Contact, as evidence of an intent to do business, could also be established if the operators made business trips, had telephone calls, or exchanged fax messages to the region. As there are many different types of businesses and business engagement, there is a wide variety of other means for proving an intent to do business within a specific region. Based on the subjective nature and wide variety of businesses and business activities, these are often determined by the court of jurisdiction on a case-by-case basis.

Unsurprisingly, the establishment of internet or online jurisdiction at the international level is not regulated the same way that internet jurisdiction may be regulated on a provincial, state, or domestic

regional level. However, the three main features for the determination of jurisdiction must still be considered in this process: judicial (or legal) jurisdiction, enforcement, and recognition.

Internet jurisdiction

Internet jurisdiction is used to determine which legal authority may hear a case, between a defendant and plaintiff, in which the alleged offence or tortious action was committed on the internet. While in typical matters, the plaintiff appeals to the court or legal authority which has jurisdiction over the geographical area in which the crime occurred, this is made much more complex when the issues at hand are committed, remotely, over the internet. In these cases, it may be difficult to determine an appropriate geographically-based jurisdiction, particularly when the originator of the illegal, tortious, or otherwise offensive action can be located in a different region or country than the individual or entity against whom the crime or offence was allegedly committed.

Usually, in cases of this nature, each country will take its own laws into consideration when determining a legal action, before considering the laws of the country in which the defendant may live. If one nation determines a crime was committed on the Internet, according to its laws, and determines that its courts have jurisdiction over the case, then that country may prosecute the offender(s), even when those involved may live in a different country.

Example: People’s Republic of China

We can see an example of the complexities which arise with the assignment of jurisdiction related to cybercrime in the codified *Chinese Criminal Law* provisions, especially Article 6, 7, 8 and 9. Specifically, Article 6 stipulates that, “Any person who commits a crime in the territory of the People’s Republic of China shall apply this law unless otherwise specifically provided by law.”

Based on the established criminal law provisions in China, Article 6 is interpreted to mean that Chinese courts have jurisdiction over criminal matters as long as one of the criminal acts or criminal consequences occurs in China. In this provision, the phrase “in China” is interpreted to include Chinese ships and aircraft outside of the territory, as well as Chinese embassies and consulates which are located abroad.

Articles 7, 8 and 9 of the *Chinese Criminal Law* respectively stipulate personal jurisdiction, protection of jurisdiction, and universal jurisdiction – all of which are considerations for determining the court of jurisdiction in criminal matters involving China.

Global costs and fatal consequences

The magnitude of the challenges associated with determining jurisdictional authority for criminal, and other activity, done using the internet, becomes glaringly clear when we look at the massive global increase in cybercriminal activity and the reported rise of cyber attacks on government, infrastructure, corporations, and individuals. On many occasions, these cyberattacks are found to have originated outside of the country in which the target is based, bringing the idea of international cyber law to the forefront of our

global legal evolution.

The costs of cybercrime include: damage and destruction of data, stolen money, lost productivity, reputational harm, theft of intellectual property, theft of personal and financial data, embezzlement, fraud and identity theft, digital forensic investigation, restoration and deletion of hacked data and systems, and post-attack disruption to the normal course of business.

In their 2021 *Internet Crime Report*, the US Federal Bureau of Investigation (FBI) reported that the number of cybercrime complaints to the Federal Bureau of Investigation rose seven per cent in 2021 to 847,376 and total money lost to cybercrime increased 64 per cent to US$6.9 billion. Among the 2021 complaints received, ransomware, business e-mail compromise schemes, and the criminal use of cryptocurrency are among the top incidents reported. In 2021 alone, business email compromise schemes resulted in 19,954 complaints with an adjusted loss of nearly US$2.4 billion. In IBM's annual *Cost of a Data Breach Report*, featuring research by the Ponemon Institute, IBM reported the highest average total data breach cost in its 17 year history, with data breach costs rising from US$3.86 million to US$4.24 million in 2021.

In 2020, Cybersecurity Ventures, a leading cybersecurity research organization, estimated the growth of global cybercrime to be about 15 per cent per year, reaching a total cost of US$10.5 trillion annually by 2025, up from US$3 trillion in 2015. This would not only represent the greatest transfer of economic wealth in history, but is also exponentially larger than the damage inflicted from natural disasters in a year, which at one point was more profitable than the global trade of all major illegal drugs combined.

Ransomware is one type of cyber attack that is especially known for being financially devastating for governments, organizations, and corporations around the world. Adding to the financial impact, a September 2020 ransomware attack on the IT systems of a major Duesseldorf hospital led to the tragic death of a patient in life-threatening condition. With IT systems crashing, the hospital was unable to access data or admit patients; surgeries were cancelled and emergency patients were taken to other hospitals for admission and treatment. For a patient in critical condition and in need of urgent medical treatment, who had to be rerouted to a hospital in a neighbouring city as a result of the ransomware attack, the hour-long delay in accessing treatment resulted in her death.

This is by far not the first time an emergency patient had to be rerouted to a different hospital as a result of a ransomware attack. According to data compiled by Emsisoft, 1,203 healthcare providers were impacted in 2021, in the United States alone. This is up from a previous investigation, also by Emsisoft, which reported that 764 US healthcare providers had been victimized by ransomware back in 2019.

Conclusion

International law structures relations among states and other international stakeholders through various prohibitions, requirements, and permissions. As such, it has provided a path for regulating global governance issues of all varieties. As nations continue to give increased attention to the governance of the internet and the technical architecture that allows the global internet to function, the role of international law in the cyber

context will continue to gain increasing prominence in our legislative discourse.

The two primary perspectives on this seem to be either for or against new law. While various states and stakeholders have suggested that existing international law is sufficient to regulate behaviour of states, others have suggested that there are gaps or inefficiencies in the existing law that require the formulation of new rules, via treaty or by an evolution of customary international law. Still within the second group, there exists a divide between those who would see a treaty created to protect states from people and those who would see the development of a treaty to protect people from states.

In our next article in this series, we will examine some of the technical challenges which are faced by governments, corporations, and organizations, in addressing the multifaceted topics of data sovereignty and digital governance in our global digital transformation.